Journal of Algebra **235,** 104–112 (2001)
doi:10.1006/jabr.2000.8467, available online at http://www.idealibrary.com on IDEAL®

On Power Integral Bases of Unramified Cyclic Extensions of Prime Degree

Humio Ichimura[1]

Yokohama, 236-0027, Japan

Communicated by Walter Feit

Received June 29, 1999

1. INTRODUCTION

By a number field, we always mean an extension over the rationals $\boldsymbol{Q}$ of finite degree. For a finite extension L/K of a number field K, one says that it has a relative power integral basis (PIB for short) when $O_L = O_K[\alpha]$ for some $\alpha \in O_L$. Here, O_L (resp. O_K) is the ring of integers of L (resp. K). We have several results on the existence or the nonexistence of PIB for L/K when $K = \boldsymbol{Q}$ and L/K is abelian, or when both K and L are certain ray class fields of an imaginary quadratic field ([2; 5; 8; 13, pp. 80–81], etc.). Except for those investigations, we have few results on PIB.

The purpose of this paper is to give (1) a proof of the following theorem on PIB (Section 2) and (2) several assertions related to this theorem (Section 3).

Let p be a fixed prime number and K a number field containing a primitive pth root of unity. We *fix* a primitive pth root ζ_p of unity and put $\pi = \zeta_p - 1$. We denote by E_K the group of units of K. We say that an extension of a number field is "unramified" when it is unramified at all finite prime divisors.

THEOREM 1 (Kawamoto, Suwa, and the author). *Under the above setting, let L/K be a cyclic extension of degree p and $G = \mathrm{Gal}(L/K)$. Then, the following two conditions are equivalent.*

[1] Partially supported by Grant-in-Aid for Scientific Research (C), Grant 11640041.

0021-8693/01 $35.00

(I) *The extension* L/K *is unramified, and* $O_L = O_K[\alpha]$ *for some* $\alpha \in O_L$ *satisfying*

$$\alpha^{\sigma} - \zeta_p \alpha \in O_K \qquad \text{for some } \sigma \in G.$$

(II) *We have* $L = K(\epsilon^{1/p})$ *for some unit* $\epsilon \in E_K$ *satisfying*

$$\epsilon \equiv u^p \mod \pi^p \text{ for some } u \in O_K. \tag{1}$$

We obtain the following corollaries immediately from Theorem 1 (and Remark 1 below).

COROLLARY 1. *Let* p *and* K *be as above. Then, an unramified cyclic extension* L/K *of degree* p *has a PIB if* $L = K(\epsilon^{1/p})$ *for some unit* $\epsilon \in E_K$.

COROLLARY 2. *Let* $p = 2$. *An unramified quadratic extension* L/K *has a PIB if and only if* $L = K(\epsilon^{1/2})$ *for some unit* $\epsilon \in E_K$.

Remark 1. For a unit $\epsilon \in E_K$, it is known (cf. Washington [16, pp. 182–183]) that $K(\epsilon^{1/p})/K$ is unramified if and only if ϵ satisfies (1).

Remark 2. Let L/K be an unramified cyclic extension of degree p. When $p \neq 2$, it follows from a theorem of Artin [1] that L/K has a relative integral basis, i.e., O_L is free over O_K. When $p = 2$, it also follows from [1] that L/K has a relative integral basis if and only if $L = K(\epsilon^{1/2})$ for some $\epsilon \in E_K$ (see also Mann [12] or Fröhlich [6]).

Remark 3. Theorem 1 was proved independently by the above three by methods different from each other. The author uses (i) some fundamental facts of algebraic number theory and (ii) a modification of an argument of Childs [4] on normal integral bases. Fuminori Kawamoto uses Okutsu's theory of "divisor polynomials," which is found in Okutsu [14] and also in Kawamoto [11]. Noriyuki Suwa uses the "unified theory" for Kummer and Artin–Schreier extensions established by Sekiguchi and Suwa [15]. The author hopes that they will publish their papers explaining their methods.

2. PROOF OF THEOREM 1

We use the same notation as in Section 1. To prove Theorem 1, we need the following well known lemma.

LEMMA 1 (cf. Iyanaga [10, p. 457]). *Let* $E/\boldsymbol{k}$ *be a finite extension of a number field* k, *and* α *an element of* O_E *with* $E = k(\alpha)$. *Define an ideal* $\mathfrak{f}_\alpha$ *of* E *by*

$$\mathfrak{f}_\alpha = \{\, \xi \in O_E \mid \omega\xi \in O_k[\alpha], \forall \omega \in O_E \,\}.$$

Then, we have $(\delta(\alpha, E/k)) = \delta(E/k) \cdot \mathfrak{f}_\alpha$. *Here,* $\delta(\alpha, E/k)$ *is the different of* α, *and* $\delta(E/k)$ *is the different of* E/k.

Proof of (I) $\Rightarrow$ (II). Let α and σ be as in the condition (I). We put

$$u = \alpha^\sigma - \zeta_p \alpha (\in O_K) \qquad \text{and} \qquad \eta = u + \pi\alpha.$$

We see that

$$\eta = u + (\zeta_p - 1)\alpha = (u + \zeta_p \alpha) - \alpha = \alpha^\sigma - \alpha.$$

On the other hand, we have $(\delta(\alpha, L/K)) = O_L$ from Lemma 1 because L/K is unramified and $O_L = O_K[\alpha]$. Therefore, we obtain $\eta \in E_L$. We see that

$$\eta^\sigma = u + \pi\alpha^\sigma = u + \pi(u + \zeta_p \alpha) = \zeta_p \eta.$$

Hence, we obtain $\epsilon = \eta^p \in E_K$ and $L = K(\epsilon^{1/p})$. Further, $\epsilon \equiv u^p \bmod \pi^p$ since $\eta = u + \pi\alpha$ and $(p) = (\pi^{p-1})$. ∎

Proof of (II) $\Rightarrow$ (I). Let ϵ and u be as in the condition (II). Put $\eta = \epsilon^{1/p}$, and choose the generator σ of G so that $\eta^\sigma = \zeta_p \eta$. We see that $\eta \equiv u \bmod \pi$ because $\eta^p \equiv u^p \bmod \pi^p$ and $(\zeta - 1) = (\pi)$ for all primitive pth roots ζ of unity. Hence, we can write $\eta = u + \pi\alpha$ for some $\alpha \in O_L$. Then, by using $\eta^\sigma = \zeta_p \eta$, we easily obtain

$$\alpha^\sigma = \zeta_p \alpha + u \qquad \text{and hence,} \qquad \alpha^\sigma - \zeta_p \alpha \in O_K.$$

From the above, we obtain inductively

$$\alpha^{\sigma^i} - \alpha = \frac{\zeta_p^{\,i} - 1}{\zeta_p - 1} \cdot \eta \in E_L \qquad (1 \le i \le p - 1),$$

and hence, $(\delta(\alpha, L/K)) = O_L$. Therefore, by lemma 1, we see that L/K is unramified and that $O_L = O_K[\alpha]$. ∎

Remark 4. The referee kindly informed the author of a variant of the above proof of Theorem 1, which is as follows. It uses a fundamental fact on Galois extensions of commutative rings given by Chase *et al.* [3] and does not use Lemma 1. In the proof of (I) $\Rightarrow$ (II), we can show that $\eta = \alpha^\sigma - \alpha$ is a unit of L from (I) and [3, Theorem 1.3(f)] without using Lemma 1. In the proof of (II) $\Rightarrow$ (I), we can show $O_L = O_K[\alpha]$ using $\alpha^\sigma - \alpha \in E_L$ and the above mentioned theorem.

3. PROPOSITIONS

One says that a finite Galois extension L/K of a number field K has a relative normal integral basis (NIB for short) when O_L is free (of rank one) over the group ring $O_K[\mathrm{Gal}(L/K)]$. In [4], Childs proved the following theorem.

THEOREM 2 (4, Theorem B). *Let p be a prime number, K a number field with $\zeta_p \in K$, and L/K a cyclic extension of degree p. Then, L/K is unramified and has a NIB if and only if $L = K(\epsilon^{1/p})$ for some unit $\epsilon \in E_K$ satisfying*

$$\epsilon \equiv 1 \mod \pi^p. \tag{2}$$

From Theorems 1 and 2, we immediately obtain the following corollary.

COROLLARY 3. *Let p and K be as in Theorem 2. Then, an unramified cyclic extension L/K of degree p has a PIB if it has a NIB.*

Let p be a fixed prime number and K a number field with $\zeta_p \in K$. For any element $\alpha \in K^\times$, $[\alpha]$ denotes the class in $K^\times/(K^\times)^p$ represented by α. In view of Theorems 1 and 2, we define subgroups $\mathscr{H}(K)$, $\mathscr{E}(K)$, $\mathscr{N}(K)$ of $K^\times/(K^\times)^p$ as follows.

$$\mathscr{H}(K) := \left\{[\alpha] \in K^\times/(K^\times)^p \mid K(\alpha^{1/p})/K \text{ is unramified}\right\}.$$

$$\begin{aligned}\mathscr{E}(K) &:= \mathscr{H}(K) \cap E_K(K^\times)^p/(K^\times)^p \\ &= \left\{[\epsilon] \in E_K(K^\times)^p/(K^\times)^p \mid \epsilon \in E_K \text{ and satisfies (1)}\right\}.\end{aligned}$$

$$\begin{aligned}\mathscr{N}(K) &:= \left\{[\alpha] \in \mathscr{H}(K) \mid K(\alpha^{1/p})/K \text{ has a NIB}\right\} \\ &= \left\{[\epsilon] \in E_K(K^\times)^p/(K^\times)^p \mid \epsilon \in E_K \text{ and satisfies (2)}\right\}.\end{aligned}$$

Here, the second equality for $\mathscr{E}(K)$ holds because of the fact in Remark 1. We also denote by $\mathscr{P}(K)$ the subset of $\mathscr{H}(K)$ consisting of classes $[\alpha]$ $(\in \mathscr{H}(K))$ for which $K(\alpha^{1/p})/K$ has a PIB. We have inclusions

$$\mathscr{N}(K) \subseteq \mathscr{E}(K) \subseteq \mathscr{P}(K) \subseteq \mathscr{H}(K).$$

We give several assertions on the above inclusions.

PROPOSITION 1. *Assume that the prime ideal $(\pi) = (\zeta_p - 1)$ of $\mathbf{Q}(\zeta_p)$ is unramified in K. Then, we have $\mathscr{E}(K) = \mathscr{N}(K)$.*

In what follows, we let p be a fixed *odd* prime number and K a CM-field with $\zeta_p \in K$. For a group X associated to K (e.g., $X = \mathscr{H}(K)$), we decompose it as $X = X^+ \oplus X^-$ by the action of the complex conjuga-

tion. We have $\mathcal{N}(K)^- = \{0\}$ by a theorem on units of CM-fields (cf. [16, Theorem 4.12]). Hence $\mathcal{N}(K) = \mathcal{N}(K)^+$.

PROPOSITION 2. *Assume that p does not divide the class number $h^+ = h(K^+)$ of the maximal real subfield K^+ of K. Then, we have $\mathcal{H}(K) = \mathcal{H}(K)^+ = \mathcal{E}(K)^+$. In particular, every unramified cyclic extension over K of degree p has a PIB.*

The following assertion follows immediately from Propositions 1 and 2.

PROPOSITION 3. *Assume that p does not divide h^+ and that the prime ideal $(\pi) = (\zeta_p - 1)$ of $\mathbf{Q}(\zeta_p)$ is unramified in K. Then, we have $\mathcal{H}(K) = \mathcal{N}(K)$. Namely, every unramified cyclic extension over K of degree p has a NIB.*

PROPOSITION 4. *Let $p = 3$. For an integer a with $a \neq 0, -2$, we put $D = D_a = 3(4a^3 + 27)$, $K = \mathbf{Q}(\sqrt{D}, \sqrt{-3})$, and $\gamma = (27 + 3\sqrt{D})/2$. Assume that D is square free. Then, the class $[\gamma]$ in $K^\times/(K^\times)^3$ is a nontrivial element of $\mathcal{H}(K)^+ \cap \mathcal{P}(K)$ (resp. $\mathcal{H}(K)^- \cap \mathcal{P}(K)$) when $D > 0$ (resp. $D < 0$).*

Remark 5. In the previous paper [9, Example 2], we gave several examples with $\mathcal{E}(K)^+ \neq \mathcal{N}(K)^+$.

Remark 6. (1) Let $p = 3$ and $K = \mathbf{Q}(\sqrt{D}, \sqrt{-3})$ with $D \in \mathbf{Z}$. Then, we have $\mathcal{E}(K)^+ = \mathcal{N}(K)^+$ by Proposition 1. (2) Under the setting of Proposition 4, assume that $D = D_a$ is positive and square free. Let r_a be the 3-rank of the ideal class group of $\mathbf{Q}(\sqrt{-3D})$, and $\mathcal{P}(K)^+$ the subgroup of $\mathcal{H}(K)$ generated by $\mathcal{H}(K)^+ \cap \mathcal{P}(K)$. In the range $-1 \leq a < 30$, D_a satisfies the assumptions and $3 \mid h^+$ when $a = 8, 10, 17, 22, 25, 29$. For these six a's, we have $\mathcal{E}(K)^+ \neq \{0\}$. For $a = 10$, we have $[\gamma] \in \mathcal{E}(K)^+$ and $r_a = 1$, hence $\mathcal{H}(K)^+ = \mathcal{P}(K)^+ = \mathcal{E}(K)^+$. Here, the first equality follows from $r_a = 1$ and the Kummer duality (see the formula (3) in Section 4). For other five a's, we have $[\gamma] \notin \mathcal{E}(K)^+$ (and $r_a = 2$), and hence $\mathcal{P}(K)^+ \neq \mathcal{E}(K)^+$.

4. PROOFS OF PROPOSITIONS 1 AND 2

Proof of Proposition 1. Let ϵ be a unit of K satisfying the condition (1). Namely, $\epsilon \equiv u^p \bmod \pi^p$ for some $u \in O_K$. From the assumption, we see that $u^n \equiv 1 \bmod \pi$ for some n with $p \nmid n$. Replacing ϵ by ϵ^n, we see that $\epsilon \equiv u^{np} \equiv 1 \bmod \pi^p$ since $(p) = (\pi^{p-1})$. Hence, we obtain $\mathcal{E}(K) = \mathcal{N}(K)$. ∎

Proof of Proposition 2. Let H/K be the maximal unramified abelian extension over K of exponent p, and $\mathfrak{h} = \mathrm{Gal}(H/K)$. The complex

conjugation ρ of K acts on $\mathfrak{h}$ in the usual way. The Kummer pairing

$$\mathfrak{h} \times \mathscr{H}(K) \to \mu_p, \qquad (\sigma, [\alpha]) \mapsto \langle \sigma, [\alpha] \rangle = (\alpha^{1/p})^{\sigma - 1}$$

is nondegenerate and satisfies

$$\langle \sigma^{\rho}, [\alpha]^{\rho} \rangle = \langle \sigma, [\alpha] \rangle^{\rho} = \langle \sigma, [\alpha] \rangle^{-1}.$$

From this, we obtain the duality

$$\mathscr{H}(K)^{\pm} \cong \mathrm{Hom}(\mathfrak{h}^{\mp}, \mu_p). \tag{3}$$

Let $A = A_K$ be the Sylow p-subgroup of the ideal class group of K. By class field theory, we have a canonical isomorphism $\mathfrak{h} \cong A/A^p$ compatible with the action of ρ. Hence, we obtain $\mathfrak{h}^+ = \{0\}$ since $p \nmid h^+$. Therefore, we see that $\mathscr{H}(K)^- = \{0\}$ and $\mathscr{H}(K) = \mathscr{H}(K)^+$ from (3). For each element $[\alpha]$ of $\mathscr{H}(K)$, there exists an ideal $\mathscr{U}$ of K such that $\mathscr{U}^p = (\alpha)$. By mapping $[\alpha]$ to the ideal class of $\mathscr{U}$, we obtain an exact sequence

$$0 \to \mathscr{E}(K) \to \mathscr{H}(K) \to A,$$

which is compatible with the action of ρ. Therefore, we obtain $\mathscr{H}(K) = \mathscr{H}(K)^+ = \mathscr{E}(K)^+$ as $p \nmid h^+$. ∎

5. PROOF OF PROPOSITION 4

We fix an integer a with $a \neq 0, -2$, and use the same notation as in Proposition 4. We put

$$K = \mathbf{Q}(\sqrt{D}, \sqrt{-3}) \qquad \text{and} \qquad L = K(\gamma^{1/3})$$

with

$$D = 3(4a^3 + 27) \qquad \text{and} \qquad \gamma = (27 + 3\sqrt{D})/2.$$

It suffices to prove that L/K is unramified and has a PIB.

We put

$$f = f_a(X) = X^3 + aX + 1.$$

As is easily seen, $f(X)$ is irreducible as $a \neq 0, -2$. The discriminant $d(f)$ of $f(X)$ is

$$d = d(f) = -(4a^3 + 27) = -D/3.$$

Let $\alpha = \alpha_1, \alpha_2, \alpha_3$ be the roots of $f(X)$. Put

$$k = \mathbf{Q}(\sqrt{d}), \qquad H = \mathbf{Q}(\alpha_1, \alpha_2, \alpha_3) = k(\alpha).$$

By the assumption of the proposition, d is square free. Therefore, we see that $\mathrm{Gal}(H/\mathbf{Q}) \cong S_3$, the symmetric group, and that H/k is unramified by Yamamura [17, Proposition]. We also see that $L = KH$ by the old formula for the roots of $f(X)$. Therefore, $O_L = O_K O_H$ by a fact on rings of integers (cf. Fröhlich and Taylor [7, pp. 124–125]). Hence, it suffices to prove the following:

LEMMA 2. *Under the above setting, the unramified extension H/k has a PIB.*

Proof of Lemma 2. Let $d = \pm \ell_1 \cdots \ell_r$ be the prime decomposition of d where the ℓ_i's are prime numbers different from each other. As d is square free, we must have

$$f(X) \equiv (X - b_i)^2 (X - c_i) \mod \ell_i$$

with $b_i \not\equiv c_i \bmod \ell_i$. Choose integers b and c so that

$$b \equiv b_i \bmod \ell_i \qquad \text{and} \qquad c \equiv c_i \bmod \ell_i \ (1 \le i \le r).$$

We put

$$\beta = (2a\alpha^2 - 3\alpha + 2abc)/\sqrt{d}$$

and prove that $O_H = O_k[\beta]$.

From the above congruence for $f(X)$, we see that

$$2a(b + c) \equiv 3 \mod d,$$

and that

$$(\sqrt{d}) = ((\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)) \mid ((\alpha - b)(\alpha - c)). \quad (4)$$

From the above, it follows that

$$\beta = \frac{2a(b + c) - 3}{\sqrt{d}}\alpha + 2a\frac{\alpha^2 - (b + c)\alpha + bc}{\sqrt{d}}$$

is an integer of H. Let σ be the automorphism of H over k sending $\alpha = \alpha_1$ to α_2. Then, we have

$$\begin{aligned} \beta - \beta^\sigma &= (\alpha_1 - \alpha_2)\{2a(\alpha_1 + \alpha_2) - 3\}/\sqrt{d} \\ &= -(\alpha_1 - \alpha_2)(2a\alpha_3 + 3)/\sqrt{d}. \end{aligned} \quad (5)$$

On the other hand,

$$(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2) = \alpha_3^2 - (\alpha_1 + \alpha_2)\alpha_3 + \alpha_1\alpha_2$$
$$= (2\alpha_3^3 - 1)/\alpha_3 = -(2a\alpha_3 + 3)/\alpha_3.$$

We see that α_3 is a unit of H since the constant term of $f(X)$ is 1. Therefore, we obtain $(\beta - \beta^\sigma) = O_H$ from (4) and (5). From this and Lemma 1, it follows that $O_H = O_k[\beta]$ as desired. ∎

Remark 7. We first showed that O_H is freely generated by 1, α, and $(\alpha^2 - (b + c)\alpha + bc)/\sqrt{d}$ over O_k by using Okutsu's theory mentioned in Remark 3. We found the β in the above proof from this.

ACKNOWLEDGMENTS

The author thanks the referee for several valuable comments, in particular for informing him of the invariant of the proof of Theorem 1.

REFERENCES

1. E. Artin, Questiones de base minimale dans la théorie des nombres algebriques, *in* "Collected Papers," pp. 229–231.
2. P. H. Cassou-Noguès and M. Taylor, Unités modulaires et monogénéité d'anneaux d'intiers, *in* "Séminaire de Théorie des Nombres, Paris, 1986–1987" (C. Goldstein, Ed.), Vol. 75, pp. 35–64, Progr. Math., Birkhäuser, Boston, 1989.
3. S. Chase, D. Harrison, and A. Rosenberg, Galois theory and Galois cohomology of commutative rings, *Mem. Amer. Math. Soc.* **52** (1965).
4. L. Childs, The group of unramified Kummer extensions of prime degree, *Proc. London Math. Soc.* **35** (1977), 407–422.
5. J. Cougnard and V. Fleckinger, Modèle Legengre d'une courbes elliptiques à multiplication complexe et monogéneité d'anneaux d'intiers II, *Acta. Arith.* **55** (1990), 75–81.
6. A. Fröhlich, The discriminants of relative extensions and the existence of integral bases, *Mathematika* **7** (1960), 15–22.
7. A. Fröhlich and M. Taylor, "Algebraic Number Theory," Cambridge Univ. Press, Cambridge, UK, 1991.
8. M. N. Gras, Condition nécessaire de monogénéité de l'anneau des entiers d'une extension abélienne de Q, *in* "Séminaire de Théorie des Nombres, Paris, 1984–1985," Progr. Math., Vol. 63, pp. 97–107, Birkhäuser, Boston, 1986.
9. H. Ichimura, On a relative normal integral basis problem over abelian number fields, *Proc. Japan Acad.* **69** (1993), 413–416.
10. S. Iyanaga (Ed.), "The Theory of Numbers," North-Holland, Amsterdam, 1975.
11. F. Kawamoto, On normal integral bases, *Tokyo J. Math.* **7** (1984), 221–231.
12. H. Mann, On integral bases, *Proc. Amer. Math. Soc.* **9** (1958), 167–172.
13. W. Narkiewicz, "Elementary and Analytic Theory of Numbers," 2nd ed., Springer-Verlag, New York, 1989.

14. K. Okutsu, Construction of integral basis, I, *Proc. Japan Acad.* **58** (1982), 47–49; II, 87–89; III, 117–119; IV, 167–169.
15. T. Sekiguchi and N. Suwa, Théorie de Kummer–Artin–Schreier, *C. R. Acad. Sci. Paris* **314** (1991), 417–420.
16. L. Washington, "Introduction to Cyclotomic Fields," Springer-Verlag, New York, 1996.
17. K. Yamamura, On unramified Galois extensions of real quadratic number fields, *Osaka J. Math.* **23** (1986), 471–478.